Omniscience principles and functions of bounded variation

Fred Richman
Florida Atlantic University
Boca Raton, FL 33431

31 July 2000

Abstract

A very weak omniscience principle is formulated, related omniscience principles are considered, and the theorem that a function of bounded variation is the difference of two increasing functions is shown to be equivalent to the omniscience principle WLPO. It is also shown that an arbitrary function (not necessarily strongly extensional) with located variation on an interval is the difference of two increasing functions.

1 A weak omniscience principle

Omniscience principles are general statements that can be proved classically but not constructively, and are used to show that other, more subject-specific statements, do not admit constructive proofs. This is done by showing that the subject-specific statement implies the omniscience principle. The strongest omniscience principle is the law of excluded middle itself.

A *Brouwerian counterexample* to a statement P is, in essence, a derivation of some omniscience principle from P. Although it is satisfying to derive a strong omniscience principle from P, it is, of course, easier to derive a weak

[1] 1991 *Mathematics Subject Classification.* Primary 03F65; Secondary 26A45
Key words and phrases. Omniscience principles, functions of bounded variation, constructive mathematics

one. So it is desirable to have some very weak omniscience principles at hand. Bishop [3], [4] formulated two omniscience principles which had been used by Brouwer:

LPO Given a binary sequence a, either $a_n = 0$ for all n, or $a_n = 1$ for some n.

LLPO Given a binary sequence a, with at most one 1, either $a_{2n} = 0$ for all n, or $a_{2n+1} = 0$ for all n.

The initials stand for the *limited principle of omniscience* and the *lesser limited principle of omniscience*. LPO may be thought of as a countable law of excluded middle.

In the absence of the countable axiom of choice, we distinguish between the (Dedekind) real numbers and the Cauchy real numbers, the latter being limits of *sequences* of rational numbers. LPO is equivalent to the statement that the Cauchy real numbers are discrete: for x and y Cauchy reals, either $x = y$ or $x \neq y$ (in the sense of apartness). LLPO is equivalent to the statement that the Cauchy real numbers are totally ordered: for x and y Cauchy reals, either $x \leq y$ or $y \leq x$. Brouwer [5] showed that the intermediate value theorem implies LLPO. In [9] a family of weakenings of LLPO were given.

LLPO$_m$ Given a binary sequence a, with at most one 1, there is r such that $a_{mn+r} = 0$ for all n. (Note that LLPO$_2$ is LLPO.)

LLPO$_\infty$ Given a binary sequence a, with at most one 1, and a partition of **N** into disjoint infinite subsets S_n, there is n such that $a_i = 0$ for all $i \in S_n$.

Palmgren [8] formulated the following principle, which is implied by LLPO$_m$ for each finite m:

L^3**PO** Given a binary sequence a, with a most one 1, there exists m and r such that $a_{r+i2^m} = 0$ for all i.

L^{3}PO says that if (t_n) is an enumeration of the nodes of a complete binary tree, and a is a binary sequence with at most one 1, then there exists n such that $a_i = 0$ whenever t_i is a descendant of t_n.

Each of these omniscience principles implies the following one, which is formulated in terms of a detachable subset of **N** containing at most one element, rather than a binary sequence with at most one 1.

- There exists a sequence S_n of infinite subsets of $\mathbf{N}$ such that $\bigcup(\mathbf{N} \setminus S_n) = \mathbf{N}$, and if A is a detachable subset of $\mathbf{N}$ containing at most one element, then there exists n such that $A \cap S_n$ is empty.

For LPO we take $S_n = \{i \in \mathbf{N} : i \neq n\}$. For LLPO$_m$ we take $S_n = n + m\mathbf{N}$. For L^{3}PO we take $S_{m,n} = n + 2^m\mathbf{N}$. For LLPO$_\infty$ we take any partition of N into countably many infinite detachable subsets. The requirement that $\bigcup(\mathbf{N} \setminus S_n) = \mathbf{N}$ makes the principle true classically for a particular sequence S_n.

There is a continuity interpretation that explains why none of these omniscience principles can be proved constructively. Let X and Y be metric spaces and $R \subset X \times Y$ a relation. We are interested in the problem of finding $y \in Y$ such that $R(x, y)$ for a given $x \in X$. Beeson [1, p. 376] says that the problem has a **stable solution at** x if there exists y such that $R(x, y)$, and if x' is close enough to x, then there exists y' close to y such that $R(x', y')$. A constructive proof of the statement "for all $x \in X$ there is $y \in Y$ such that $R(x, y)$," would seem to require that there be a stable solution at x for each $x \in X$. Otherwise the problem would be **ill posed** in the sense that, at some point, small changes in the data would require large changes in the solution. This would presumably make computation of that solution impossible.

The problem posed by • is ill posed in this sense. Given a sequence S_n as above, let X be the set of all binary sequence with at most one 1, let Y be $\mathbf{N}$, and let $R(x, n)$ mean $x_n = 0$. The most interesting point x in X is the all-zeros sequence. For this value of x, we have $R(x, n)$ for any natural number n. But to be close to n is to be equal to n. So for the problem to have a stable solution at x it would have to be the case that any $x' \in X$ sufficiently close to x would satisfy $R(x', n)$. But that's not true because S_n is infinite.

Note that we cannot replace the sequence of infinite subsets by an arbitrary set of infinite subsets. Indeed, if A is a detachable subset of $\mathbf{N}$ containing at most one element, then there exists an infinite subset S of $\mathbf{N}$ such that $A \cap S$ is empty. Just take $S = \mathbf{N} \setminus A$.

Constructively, we think of every function as being computable. Church's thesis, in this context, says that every function from $\mathbf{N}$ to $\mathbf{N}$ is recursive. In the presence of Church's thesis, we can actually refute •. That is the import of the following theorem.

Theorem 1 *Let $S \subset \mathbf{N} \times \mathbf{N}$ be a recursive subset. Suppose that $S_n = \{i \in$*

$\mathbf{N} : (i,n) \in S\}$ is infinite for each n. Then there is a total recursive function a_j^i, in the two variables i and j, such that

1. *Each a_*^i is a binary sequence with at most one* 1
2. *If f is a total recursive function, then there exists i and j such that $a_j^i = 1$ and $j \in S_{f(i)}$.*

Proof. Let φ_n be the partial recursive function computed by the n-th Turing machine. Define the total recursive function a_j^i by setting $a_j^i = 1$ exactly when j is the least integer in S_n such that $\varphi_i(i) = n$ in at most j steps. By the s-m-n theorem there is a total recursive function g such that $\varphi_{g(i)}(k) = f(i)$ for all i and k (so $\varphi_{g(i)}$ is constant). By the recursion theorem, there is i_0 such that $\varphi_{g(i_0)} = \varphi_{i_0}$. Therefore $\varphi_{i_0}(i_0) = f(i_0)$. As $S_{f(i_0)}$ is infinite, there exists $j \in S_{f(i_0)}$ such that $\varphi_{i_0}(i_0) = f(i_0)$ in at most j steps. So there exists $j \in S_{f(i)}$ such that $a_j^{i_0} = 1$. ■

In light of this theorem, there is no hope of finding a constructive proof of •. So a derivation of • from some statement constitutes a Brouwerian counterexample to that statement.

The *weak limited principle of omniscience* (see [7]) is

WLPO Given a binary sequence a, either $a_n = 0$ for all n, or it is impossible that $a_n = 0$ for all n.

Brouwer alludes to this principle in [6, Page 42]. WLPO is equivalent to the statement that the Cauchy real numbers are *weakly discrete*, that is, discrete under the denial inequality: if x and y are Cauchy reals, then either $x = y$ or $\neg(x = y)$. Clearly WLPO is implied by LPO and implies LLPO. We will see in Theorem 4 that WLPO is equivalent to a standard theorem about functions of bounded variation.

2 Equivalent formulations of LLPO$_m$

The omniscience principle LLPO$_m$, for finite m, can appear in different forms. Consider the triply indexed family $P_{m,n,k}$ of statements:

> If $S_1, \ldots, S_n$ are disjoint infinite subsets of $\mathbf{N}$, and A is a detachable subset of $\mathbf{N}$ of cardinality at most m, then $A \cap S_i$ is empty for at least k values of i.

We will show that $P_{m,n,k}$ is equivalent to LLPO_t where $t = \lceil (n-k+1)/m \rceil$. For $P_{m,n,k}$ to be classically true, we need to require that $t > 1$.

Theorem 2 *The statements $P_{m,n,k}$ and $P_{m,n+1,k+1}$ are equivalent.*

Proof. Assume $P_{m,n,k}$ and consider disjoint infinite subsets $S_1, \ldots, S_n, S_{n+1}$ and a detachable set A containing at most m elements. Each n-element subset of $\{1, 2, \ldots, n+1\}$ contains k good indices. So there have to be $k+1$ good indices. Conversely, assume $P_{m,n+1,k+1}$ and consider disjoint infinite subsets $S_1, \ldots, S_n$. Split S_i in two. You get k good indices. ■

So we may as well assume that $k = 1$, and let $P_{m,n} = P_{m,n,1}$. That is $P_{m,n}$ is the statement

> If $S_1, \ldots, S_n$ are disjoint infinite subsets of $\mathbf{N}$, and A is a detachable subset of $\mathbf{N}$ of cardinality at most m, then $A \cap S_i$ is empty for some i.

Note that $P_{1,n}$ is LLPO_n. We need to require that $m < n$ for $P_{m,n}$ to be classically true.

Theorem 3

1. *$P_{m,n}$ implies $P_{m,n+1}$.*
2. *$P_{km,kn}$ implies $P_{m,n}$*
3. *$P_{1,k}$ is equivalent to $P_{m,n}$ if $(k-1)m < n \leq km$ (that is, if $k = \lceil n/m \rceil$).*

Proof. Clearly (1) holds. To show (2), suppose we have disjoint infinite subsets $S_1, \ldots, S_n$ and a detachable subset A of cardinality at most n. Make k identical copies of this situation. By $P_{km,kn}$, one of the kn infinite subsets is disjoint from the union of the k copies of A. Hence some S_i is disjoint from A.

To show (3), suppose $(k-1)m < n \leq km$ with $k > 1$. To show that $P_{1,k}$ implies $P_{m,n}$, let $S_1, \ldots, S_n$ be disjoint infinite subsets of $\mathbf{N}$, and A a detachable subset of $\mathbf{N}$ of cardinality at most m. Write A as a union $A_1 \cup \cdots \cup A_m$ where each A_i is a detachable subset of $\mathbf{N}$ of cardinality at most 1. By repeated application of $P_{1,k}$, there is a subset J_i of $\{1, 2, \ldots, n\}$ of cardinality $n - k + 1$ such that $A_i \cap S_j$ is empty for each $j \in J_i$. So each subset J_i omits $k-1$ elements of $\{1, 2, \ldots, n\}$. Because $(k-1)m < n$, the intersection of the J_i is nonempty. If j is in that intersection, then $A \cap S_j$ is empty. To show, conversely, that $P_{m,n}$ implies $P_{1,k}$, note by (1) that $P_{m,n}$ implies $P_{m,km}$, which implies $P_{1,k}$ by (2).■

3 Functions of bounded variation

A **subdivision** x of an interval $[a, b]$ is a sequence

$$a \leq x_1 \leq x_2 \leq \cdots \leq x_m \leq b$$

The numbers x_i are said to be **elements** of x. A subdivision y is a **refinement** of a subdivision x if each element of x is an element of y.

If f is a function on the interval $[a, b]$, then the variation of f over x is defined to be

$$V_x = \sum_{i=0}^{m-1} |f(x_{i+1}) - f(x_i)|$$

The **variation** of f on $[a, b]$ is defined to be the supremum of V_x as x varies over all subdivisions of $[a, b]$. This supremum always exists as a generalized real number [10]; when it exists as a real number, so we can find arbitrarily close rational approximations to it, we say that the variation is **located**. Any function with a located variation is the difference of two increasing functions (Corollary 8). However, if the variation of f is just *bounded*, then we cannot necessarily write f as the difference of two increasing functions.

In the proof of the next theorem we will use the notion of a *weak least upper bound*. This notion is of interest only because, for one half of the theorem, we assume WLPO. We say that a real number b is a **weak least upper bound** of a set S provided that $a \geq s$ for all s in S if and only if $a \geq b$. Clearly weak least upper bounds are unique. The weakness comes from the fact that we do not require, for $a < b$, that we can find s in S such that $s > a$. The stronger concept is much more useful.

Theorem 4 *If every uniformly continuous function on* $[0, 1]$ *of bounded variation is the difference of two increasing functions, then WLPO holds. The converse holds in the presence of the axiom of countable choice.*

Proof. First note that, for every $n \geq 1$ there a uniformly continuous function g_n of variation 1 on $[0,1]$, bounded by $1/n$, such that $g(x) = 0$ outside $[0, 1/n]$. If $a_1, a_2, \ldots$ is a binary sequence with at most one 1, then

$$\sum_{n=1}^{\infty} a_n g_n$$

converges uniformly to a function f whose variation is bounded by 1. Suppose $f = h - k$ where h and k are increasing functions. Then the variation of f on any interval is bounded by the variation of the increasing function $\lambda = h + k$ on that interval. We may assume that $\lambda(0) = 0$. Set

$$s = \sum_{n=0}^{\infty} \frac{a_n}{n}$$

If $a_n = 1$, then $s = 1/n$ and $f = g_n$, so $\lambda(s) \geq 1$. So if $\lambda(s) < 1$, then $a_n = 0$ for all n. If $\lambda(s) > 0$, then s can't be zero, so the a_n can't all be 0.

For the converse, suppose that WLPO holds and let f be a uniformly continuous function on $[0,1]$ of bounded variation. Because of WLPO, and the axiom of countable choice, we can compute the weak least upper bound of the sums

$$\sum_{i=0}^{n-1} |f(x_{i+1}) - f(x_i)|$$

over all finite sequence of rational numbers $x_0 \leq \cdots \leq x_n$ in any subinterval of $[0,1]$, for all n. Because f is uniformly continuous, the same b works if we allow the x_i to be real. Roughly speaking, we can compute the variation of f without being able to show that it *is* the variation, which would require finding sums that were arbitrarily close to it.

Let $h(x)$ be the variation of f (in this weak sense) on the interval $[0, x]$. Then $h(t) - h(s)$ is the variation of f on the interval $[s, t]$, so h and $h - f$ are increasing functions. ■

Note that if we demand continuity of the increasing functions, then we get LPO: choose n so that $\lambda(1/n) - \lambda(0) < 1$.

4 Functions of located variation

A function is f is **strongly extensional** if $a \neq b$ whenever $f(a) \neq f(b)$. Pointwise continuous functions are strongly extensional. In [2] it was shown that every strongly extensional function with located variation is the difference of increasing functions. We extend this result to arbitrary functions.

Theorem 5 *Let f be a function on $[a, b]$. Let x be any subdivision of $[a, b]$ and c any element of $[a, b]$. Then there exists a subdivision z of $[a, b]$, containing c and any $x_j \leq c$, such that $V_z \geq V_x$.*

Proof. The desired subdivision z is

$$x_1 \wedge c \leq x_2 \wedge c \leq \cdots \leq x_m \wedge c \leq c \leq x_1 \vee c \leq x_2 \vee c \leq \cdots \leq x_m \vee c.$$

The only question is whether $V_z \geq V_x$.

Clearly if P and Q are propositions such that Q and $\neg(Q \,\&\, P)$ hold, then $\neg P$ holds. So, for any propositions P and Q we have

$$\neg(Q \,\&\, P) \,\&\, \neg\neg P \Rightarrow \neg Q.$$

In particular, if $\neg\neg Q$ and $\neg\neg P$, then $\neg\neg(Q \,\&\, P)$, and, by induction, the same holds for a conjunction of any finite number of propositions.

Now Let Q be the proposition $V_y < V_x$. We want to show $\neg Q$. Let P_i be the proposition

$$x_i \neq c \text{ or } x_i = c$$

and P be the proposition "$P_1 \,\&\, P_2 \,\&\, \ldots \,\&\, P_m$". Clearly $\neg\neg P_i$ for each i, so $\neg\neg P$. Therefore $\neg Q$. ∎

Corollary 6 *Let x and y be subdivisions of $[a, b]$. Then there is a refinement z of y such that $V_z \geq V_x$.*

Proof. Let y be $y_1 \leq \cdots \leq y_n$. The theorem is the case $n = 1$ (alternatively, the case $n = 0$ is trivial). Let y' be $y_1 \leq \cdots \leq y_{n-1}$. We may assume, by induction, that there is a refinement z' of y' such that $V_{z'} \geq V_x$. From the theorem, there is a subdivision z containing y_n and each $z'_j \leq y_n$ (hence a refinement of y) such that $V_z \geq V_{z'}$. ∎

Corollary 7 *Let f be a function on $[a, b]$ and c an element of $[a, b]$. If the variation of f is located on $[a, b]$, then it is located on $[a, c]$ and $[c, b]$.*

Proof. Let V be the variation of f on $[a,b]$, and $\varepsilon > 0$. Then there exists a subdivision x of $[a,b]$, containing c, such that $V_x > V - \varepsilon$. Let x be $y_1 \leq \cdots \leq y_m = c = z_1 \leq \cdots \leq z_n$. Then the variation of f on $[a,c]$ is less than $V_y + \varepsilon$, and the variation of f on $[c,b]$ is less than $V_z + \varepsilon$. ■

Corollary 8 *Let f be a function on $[a,b]$. If the variation of f is located on $[a,b]$, then f is the difference of two increasing functions.*

Proof. Let $g(c)$ be the variation of f on $[a,c]$. For $c < d$ in $[a,b]$ the difference $g(d) - g(c)$ is the variation of f on $[c,d]$. Thus g is increasing. Moreover, $g(d) - g(c) \geq f(d) - f(c)$, so $g - f$ is increasing. ■

Strong extensionality says that if $f(a) \neq f(b)$, then $a < b$ or $b < a$. Somewhat surprisingly, the following weaker form always holds.

Theorem 9 *If $f(a) \neq f(b)$, then $a \leq b$ or $b \leq a$*

Proof. As $f(a) \neq f(b)$, either $f(a) \neq f(a \vee b)$ or $f(b) \neq f(a \vee b)$. Suppose $f(a) \neq f(a \vee b)$. As $a > b$ implies $f(a) = f(a \vee b)$, it follows that $a \leq b$. Similarly, if $f(b) \neq f(a \vee b)$, then $b \leq a$. ■

Corollary 10 $|f(a \vee b) - f(a \wedge b)| = |f(a) - f(b)|$

Proof. If $|f(a \vee b) - f(a \wedge b)| \neq |f(a) - f(b)|$, then either

$$|f(a \vee b) - f(a \wedge b)| \neq 0 \text{ or } |f(a) - f(b)| \neq 0.$$

In the latter case, $a \leq b$ or $b \leq a$, so the desired equation holds. So suppose $f(a \vee b) \neq f(a \wedge b)$. Then either $f(a) \neq f(a \vee b)$ or $f(a) \neq f(a \wedge b)$. Suppose the former. If $a > b$, then $f(a) = f(a \vee b)$, so $a \leq b$, and the equation holds. Similarly, if $f(a) \neq f(a \wedge b)$, then $b \leq a$ and the equation holds. ■

References

[1] Beeson, Michael J., *Foundations of constructive mathematics*, Springer-Verlag, 1985

[2] Bridges, Douglas S., A constructive look at functions of bounded variation, *Bull. London. Math. Soc.* **32** (2000) 316–324.

[3] BISHOP, ERRETT, *Foundations of constructive analysis*, McGraw-Hill 1967

[4] ________________, *Schizophrenia in contemporary mathematics*, 1973, in *Errett Bishop: Reflections on him and his research*, *Contemp. Math.*, **39** American Mathematical Society 1985

[5] BROUWER, L.E.J., Volition, knowledge, language, in *L.E.J. Brouwer, Collected works I*, A. Heyting, ed., North-Holland 1975, 443–446

[6] ________________, *Brouwer's Cambridge lectures on intuitionism*, D. Van Dalen, ed., Cambridge University Press 1981

[7] MANDELKERN, MARK, *Constructive continuity*, Memoirs of the American Mathematical Society, Number 277, 1983.

[8] PALMGREN, ERIK, *Sheaf-theoretic nonstandard analysis: constructive aspects*, Uppsala University Department of Mathematics Report 1996:28

[9] RICHMAN, FRED, Polynomials and linear transformations, *Linear Algebra and its Applications*, **131** (1990) 131–137

[10] ________________, Generalized real numbers in constructive mathematics, *Indag. Math.* **9** (1998) 595–606.